



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/642,878	08/21/2000	Stephen Michael Matyas JR.	5577-203	8116
20792	7590	09/22/2004	EXAMINER	
MYERS BIGEL SIBLEY & SAJOVEC				BROWN, CHRISTOPHER J
PO BOX 37428				
RALEIGH, NC 27627				
				ART UNIT
				PAPER NUMBER
				2134

DATE MAILED: 09/22/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/642,878	MATYAS ET AL.
	Examiner	Art Unit
	Christopher J. Brown	2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 24 October 2000.
- 2a) This action is **FINAL**. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-84 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-84 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 21 August 2000 is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>7/16/2004</u> . | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 5, and 6 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 5 states “generating the plurality of personal keys from the current passphrase associated with the plurality of files” It is not certain whether the applicant means that *one* passphrase generates *multiple* keys, or that a plurality of corresponding passphrases generate a plurality of corresponding keys. The Examiner is interpreting the claim as the latter statement.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-7, 29-35, and 57-63 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lineham US 5,495,533 in view of Ote US 6,023,506.

As per claims 1, 2, 29, 30, 58, and 59, Lineham teaches a file encryption system that encrypts a file encryption key with a personal key (control key), (Col 8 lines 57-65). Lineham teaches storing the file encryption key in a header and associating that header with the encrypted file, (Col 8 lines 50-60). Lineham teaches a file server to store encrypted files, (Col 6 lines 53-55). Lineham fails to teach the personal key is generated from a pass phrase.

Ote teaches that a key may be generated using a pass phrase (password), (Col 4 lines 35-39, Col 5 lines 8-13). It would have been obvious to one of ordinary skill in the art to use the key generated by a pass phrase from Ote to the file encryption system of Lineham because a pass phrase is easy to remember and allows the user to avoid management of encryption keys, (Ote Col 2 lines 65-68 to Col 3 lines 1-4).

As per claims 3, 31, and 59, Lineham teaches that the personal key (control key) is changed periodically and re-encrypts file encryption keys, (Col 9 lines 3-10).

As per claims 4, 32, and 60, Lineham teaches a file server to store encrypted files, (Col 6 lines 53-55).

As per claims 5, 33, and 61 It is inherent that for multiple files, multiple keys will be used for encryption, and multiple headers will be created.

As per claims 6, 34, and 62 Lineham teaches a file server to store encrypted files, (Col 6 lines 53-55).

As per claims 7, 35, and 63, Lineham teaches a file decryption by utilizing a key to decrypt the key encryption key in the header, and using said key encryption key to

decrypt said file, (Col 9 lines 55-59). Lineham fails to teach the personal key is generated from a pass phrase.

Ote teaches that a key may be generated using a pass phrase (password), (Col 4 lines 35-39, Col 5 lines 8-13).

Claims 8, 9, 10, 36, 37, 38, 64, 65 and 66 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lineham US 5,495,533 in view of Ote US 6,023,506 in view of Nguyen US 5,638,448.

As per claims 8, 36, and 64, The previous Lineham-Ote combination does not teach combining identification and passphrases to create a personal key.

Nguyen teaches combining identification and passphrases to create a key, (Col 4 lines 12-16). It would have been obvious to one of ordinary skill in the art to add the personal key generation of Nguyen to the Encryption system of Lineham-Ote because the identification added increases security.

As per claims 9, 10, 37, 38, 65, and 66 Lineham teaches a file server to store encrypted files, (Col 6 lines 53-55). It is inherent that a user would store a file based on the type of storage they request.

Claims 11-17, 39-45, and 67-73 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lineham US 5,495,533 in view of Ote US 6,023,506 in view of Lewis US 5,734,819

As per claim 11, 13, 39, 41, 67, and 69 Lineham teaches including a message authentication code in the header associated with a file, (Col 10 lines 13-18). Lineham fails to teach a key to create the message authentication code.

Lewis teaches that a key is to be used in operation of the message authentication code. Lewis teaches the key is to be kept secret. It would be inherent to encrypt the key for transit with the message authentication code thus keeping it safe, (Col 2 lines 20-46). It would have been obvious to one of ordinary skill in the art to include the key of Lewis with the system of line ham because the key increases the security of the message authentication code.

As per claims 12, 40, and 68 Lineham teaches a file server to store encrypted files, (Col 6 lines 53-55).

As per claims 14, 42, 70, Lineham teaches hashing to create a verification value (header message authentication code), (Col 8 lines 62-65). Lineham teaches the message authentication code is encrypted with the personal key (Col 8 lines 62-65). Lineham fails to teach a key to create the message authentication code.

Lewis teaches that a key is to be used in operation of the message authentication code. Lewis teaches the key is to be kept secret. It would be inherent to encrypt the key for transit with the message authentication code thus keeping it safe, (Col 2 lines 20-46). It would have been obvious to one of ordinary skill in the art to include the key of Lewis with the system of line ham because the key increases the security of the message authentication code.

As per claims 15, 43, and 71 Lineham teaches a file server to store encrypted files, (Col 6 lines 53-55).

As per claims 16, 44, and 72 Lineham teaches validating the header message authentication code in the process of file decryption, (Col 9 lines 47-50). Although not explicitly stated, it is inherent that another mac would have to be created by hashing the header including the keys, and comparing to the original mac.

As per claims 17, 45, and 73 Lineham teaches a message authentication code for the encrypted file, (Col 10 lines 13-21). Although not explicitly stated, it is inherent that another mac would have to be created by hashing the file and comparing to the original mac.

Lewis explicitly teaches the mac authentication process, (Col 2 lines 34-47).

Claims 18-20, 46-48, and 74-76 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lineham US 5,495,533 in view of Ote US 6,023,506 in view of Davis US 5,805,712

As per claims 18, 20, 46, 48, 74, 76 the prior Lineham-Ote combination teaches an encryption system with a personal symmetric key, and a header. The combination does not teach public key cryptography.

Davis teaches encryption and decryption through the use of a key pair, (Col 2 lines 3-6).

Davis teaches a public key encrypts, while a private key decrypts, (Col 2 lines 5-10).

Art Unit: 2134

It would have been obvious to one of ordinary skill in the art to replace the personal symmetric key system of the Lineham-Ote combination with the public key system of Davis because the public key system alleviates key management associated with symmetric key cryptography, (Davis Col 2 lines 10-13).

As per claims 19, 47, and 75 Lineham teaches a file server to store encrypted files, (Col 6 lines 53-55).

Claims 21-28, 49-56, and 77-84 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lineham US 5,495,533 in view of Ote US 6,023,506 in view of Davis US 5,805,712 in view of Lewis US 5,734,819

As per claims 21, 24, 49, 52, 77, and 80, As previously stated in this office action, the Lineham-Ote combination teaches an encryption system that encrypts a file encryption key, includes it in the header, and also includes a message authentication code, (Col 8 lines 56-65, Col 10 lines 13-20).

Lewis teaches that a key is to be used in operation of the message authentication code. Lewis teaches the key is to be kept secret. It would be inherent to encrypt the key for transit with the message authentication code thus keeping it safe, (Col 2 lines 20-46). It would have been obvious to one of ordinary skill in the art to include the key of Lewis with the system of line ham because the key increases the security of the message authentication code.

Art Unit: 2134

Davis teaches encryption and decryption through the use of a key pair, (Col 2 lines 3-6).

Davis teaches a public key encrypts, while a private key decrypts, (Col 2 lines 5-10).

It would have been obvious to one of ordinary skill in the art to replace the personal symmetric key system of the Lineham-Ote combination with the public key system of Davis because the public key system alleviates key management associated with symmetric key cryptography, (Davis Col 2 lines 10-13).

As per claims 22, 50, and 78 Lineham teaches a file server to store encrypted files, (Col 6 lines 53-55).

As per claims 23, 27, 51, 55, 79, and 83, Lineham teaches hashing to create a verification value (header message authentication code), (Col 8 lines 62-65). Lineham teaches the message authentication code is encrypted with the personal key (Col 8 lines 62-65).

Lineham teaches validating the header message authentication code in the process of file decryption, (Col 9 lines 47-50). Although not explicitly stated, it is inherent that another mac would have to be created by hashing the header including the keys, and comparing to the original mac.

Lineham fails to teach a key to create the message authentication code.

Lewis teaches that a key is to be used in operation of the message authentication code.

Lewis teaches the key is to be kept secret. It would be inherent to encrypt the key for transit with the message authentication code thus keeping it safe, (Col 2 lines 20-46). It would have been obvious to one of ordinary skill in the art to include the key of Lewis

Art Unit: 2134

with the system of line ham because the key increases the security of the message authentication code.

Davis teaches encryption and decryption through the use of a key pair, (Col 2 lines 3-6).

Davis teaches a public key encrypts, while a private key decrypts, (Col 2 lines 5-10).

It would have been obvious to one of ordinary skill in the art to replace the personal symmetric key system of the Lineham-Ote combination with the public key system of Davis because the public key system alleviates key management associated with symmetric key cryptography, (Davis Col 2 lines 10-13).

As per claims 25, 53, 81, Lineham teaches hashing to create a verification value (header message authentication code), (Col 8 lines 62-65). Lineham teaches the message authentication code is encrypted with the personal key (Col 8 lines 62-65). Lineham fails to teach a key to create the message authentication code. Lineham does not disclose public key cryptography.

Lewis teaches that a key is to be used in operation of the message authentication code.

Lewis teaches the key is to be kept secret. It would be inherent to encrypt the key for transit with the message authentication code thus keeping it safe, (Col 2 lines 20-46). It would have been obvious to one of ordinary skill in the art to include the key of Lewis with the system of line ham because the key increases the security of the message authentication code.

Davis teaches encryption and decryption through the use of a key pair, (Col 2 lines 3-6).

Davis teaches a public key encrypts, while a private key decrypts, (Col 2 lines 5-10).

It would have been obvious to one of ordinary skill in the art to replace the personal symmetric key system of the Lineham-Ote combination with the public key system of Davis because the public key system alleviates key management associated with symmetric key cryptography, (Davis Col 2 lines 10-13).

As per claims 26, 54, and 82 Lineham teaches a file server to store encrypted files, (Col 6 lines 53-55).

As per claims 28, 56, and 84, Lineham teaches a message authentication code for the encrypted file, (Col 10 lines 13-21). Although not explicitly stated, it is inherent that another mac would have to be created by hashing the file and comparing to the original mac.

Lewis explicitly teaches the mac authentication process, (Col 2 lines 34-47).

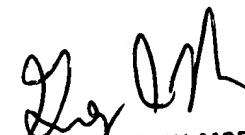
Conclusion

3. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher J Brown whose telephone number is (571)272-3833. The examiner can normally be reached on (571)272-3833. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on (571)272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2134

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher J Brown



GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100